



Ejercicio Práctico de Portafolio

Análisis de Amenazas y Vulnerabilidades en Aplicaciones Web


Objetivo del ejercicio

Aplicar conocimientos fundamentales de ciberseguridad para **identificar visualmente amenazas y vulnerabilidades** en una aplicación web pública, utilizando únicamente herramientas de inspección del navegador.

Instrucciones

1. Selecciona una aplicación web real

Escoge cualquier sitio web institucional, académico, gubernamental o empresarial que esté disponible públicamente.

 **Importante:** Este es un ejercicio de **análisis pasivo**, exclusivamente observacional. No está permitido realizar pruebas activas, ataques, inyecciones ni alteraciones del sistema.

2. Realiza una exploración técnica en modo desarrollador

Abre el **modo desarrollador del navegador** (F12 o clic derecho → “Inspeccionar”) y navega por la aplicación como un usuario regular.

Observa y documenta:

- Formularios disponibles (login, contacto, búsqueda, comentarios)
- URLs y parámetros visibles
- Comportamiento ante errores
- Consola y pestaña de red

- Cookies almacenadas
 - Códigos de estado HTTP (pestaña “Red”)
-

3. Identifica amenazas potenciales

Analiza y documenta al menos:

- **3 amenazas externas** (como phishing, XSS, malware)
 - **2 amenazas internas** (como mal uso de privilegios, exposición de rutas administrativas)
-

4. Detecta vulnerabilidades visibles

Sin ejecutar ataques, identifica **3 posibles vulnerabilidades**, como:

- Exposición de rutas sensibles (por URL)
 - Cookies sin `httpOnly` o `secure`
 - Formularios sin token CSRF
 - Parámetros en URLs que podrían ser manipulados (`?id=1`)
-

5. Completa la tabla de análisis

Utiliza esta tabla para documentar lo observado:

Nº	Tipo (Amenaza/Vulnerabilidad)	Descripción	Riesgo Potencial	Medida de Mitigación
1	Vulnerabilidad (Cookies inseguras)	No se usa httpOnly en cookie de sesión	Robo de sesión	Configurar atributos seguros en cookies

6. Propón buenas prácticas

Redacta al menos **5 buenas prácticas** de seguridad web que podrían aplicarse al sitio analizado, como:

- Validación estricta de entrada del usuario
 - Implementación de HTTPS obligatorio
 - Cookies con atributos seguros
 - Gestión adecuada de errores
 - Control de acceso por roles
-

7. Reflexión final

Redacta una reflexión personal (mínimo 150 palabras) sobre:

- ¿Qué tan expuesta está la aplicación evaluada?
 - ¿Qué aspectos te sorprendieron durante el análisis?
 - ¿Qué impacto tendría aplicar las buenas prácticas que recomendaste?
-

Entregables

- Informe en formato Word o PDF que contenga:
 - Capturas de pantalla de la inspección
 - Tabla completa de amenazas y vulnerabilidades
 - Lista de buenas prácticas sugeridas
 - Reflexión final
-

Herramientas permitidas

- Cualquier navegador web moderno (Chrome, Firefox, Edge)

- Herramientas nativas de inspección (modo desarrollador)

Instrumento de Evaluación – Ejercicio Práctico

Análisis de Amenazas y Vulnerabilidades en Aplicaciones Web

Puntaje total: 10 puntos

Nota mínima para aprobar: 6 puntos

Criterio Evaluado	Puntaje
Selección de aplicación web válida	1 pt
Uso correcto del modo desarrollador e inspección de elementos	2 pts
Identificación de amenazas (mínimo 5, bien explicadas)	2 pts
Identificación de vulnerabilidades visibles (mínimo 3)	2 pts
Tabla de análisis completada (al menos 3 entradas)	1 pt
Propuesta de buenas prácticas de seguridad (mínimo 5)	1 pt
Reflexión final redactada (mínimo 150 palabras)	1 pt
